Fall 2016

User Behavior Analytics

Haylee Brewer

User Behavior Analytics

Haylee Brewer – University of Texas at Tyler

Introduction

According to the Tech Target (2015) website, "User behavior analytics is the tracking, collecting and assessing of user data and activities using monitoring systems." User behavior analytics is composed of three fundamental elements, which includes data collection, analysis and results. The information gathered is stored and analyzed meticulously for normal and abnormal behavior patterns. Abnormal or suspicious activities will raise a red flag, which will allow for an action plan to take place. This plan will be composed of a prevention method that will secure the data system. Abnormal behavior is not always considered a risk. Such behavior must be monitored and evaluated before it is considered "risky" and action is taken. Anomaly detection helps to determine what is normal and what is not, as well as detect attacks, internal misuse and operation issues. There are many cases where companies do not catch these suspicious behaviors in time and the security system is breached or shut down. Using the results obtained from a user behavior analysis can detect malicious behavior, such as financial fraud, sabotage, and the appropriation of trade secrets. The main objective of user behavior analytics is to notice and prevent the occurrence of anomalous behavior and its ramifications.

Software

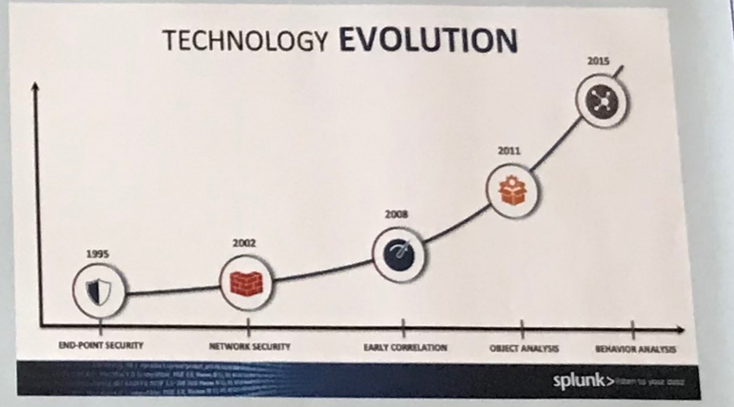
Many types of user behavior tools and software programs are available for companies to purchase. TechTarget's article over user behavioral analytics (2015) states, "these tools don't take defensive action themselves but merely provide security operators with the insight to determine whether action is needed." Companies must determine what UBA software would best fit their needs. Software differentiators range from data sources to delivery mechanisms. Data sources refers to the types of data and files the UBA tool integrate with, examples include excel, firewalls, and routers. Time of results is also important to consider when choosing the right tool. This refers to the time it takes the tool to produce actionable results. Delivery mechanism refers to how the tool is delivered, such as through software-only, an appliance, or cloud-based (TechTarget).

Cases

In February of 2015, health plan Anthem Inc. suffered a major hacker attack. This company was phished, which is a type of attack through email that encourages employees to enter personal information on an unsecure website. Anthem Inc. could have taken multiple actions to recognize an attack sooner or even prevent one from taking place. According to the Data Breach Today (2016), "One huge takeaway from the Anthem breach is that we all truly need to subscribe to continuous monitoring in our environment and understanding user behavior – especially privileged users. Had there been some targeted monitoring of what the privileged users were doing at Anthem, this suspicious behavior would have possibly been detected much sooner." Anthem should use user behavior analysis to try and prevent a breach like this from happening again.

User behavior analysis can be beneficial for companies that sell products online. A normal behavior is defined by a customer going online and searching through multiple products and then making a purchase. Malicious behavior would raise a red flag if a user were to have failed login attempts, goes directly to one product, and then changes the shipping address before completing the purchase. The amount of time a user spends browsing, their history, and how they browse are all online shopping behaviors that can be critical to preventing and detecting fraud (Secured Touch). Login failures are one of the most commonly detected behaviors.

History



Conclusion

User behavior analytics is a very useful tool used to protect businesses and sensitive information. Accounting information systems and consumer data logging systems are in need of security to shield against attackers and thieves. The breach of company information can be extremely harmful in certain venues, such as a hospital or financial institution. In the future, behavioral analysis will most likely be adapted to devices, such as a smartphone's operating system, not just apps that use the technology. Fraudsters often find ways around security measures, but it's not possible to mimic every aspect of a user's behavior (Secured Touch). Different types of software are available for the various types of entities.

References:

Behavioral Analysis: The Future of Fraud Prevention – Secured Touch. (2015). Retrieved June 04, 2016, from http://securedtouch.com/behavioral -analysis-the-future-of-fraud-prevention/

Johnson, J. (2015, May). User behavioral analytics tools can thwart security attacks. Retrieved June 04, 2016, from http://searchsecurity.techtarget.com/feature/User-behavioral-analytics-tools-can-thwart-security-attacks

Leverage machine learning using splunk user behavioral analytics. (2015, December 4). Retrieved March 10, 2016, from http://www.slideshare.net/Splunk/lever age-machine-learning-using-splunk-user-behavioral-analytics

McGee, M. (2015, February 26). Anthem Breach: Lessons One Year Later. Retrieved March 10, 2016, from http://www.databreachtoday.com/anthem-breach-lessons-one-year-later-a-8897

What is user behavior analytics (UBA)? - Definition from Whatls.com. (2015, September). Retrieved March 10, 2016, from http://searchsecurity.techtarget.com/definition/user-behavior-analytics-UBA

Risk Fabric - User Behavior Analytics (UEBA). (n.d.). Retrieved April 18, 2016, from http://baydynamics.com/risk-fabric/